DMARC

einfach
einrichten

Kurze Fakten zu DMARC

Was ist DMARC?

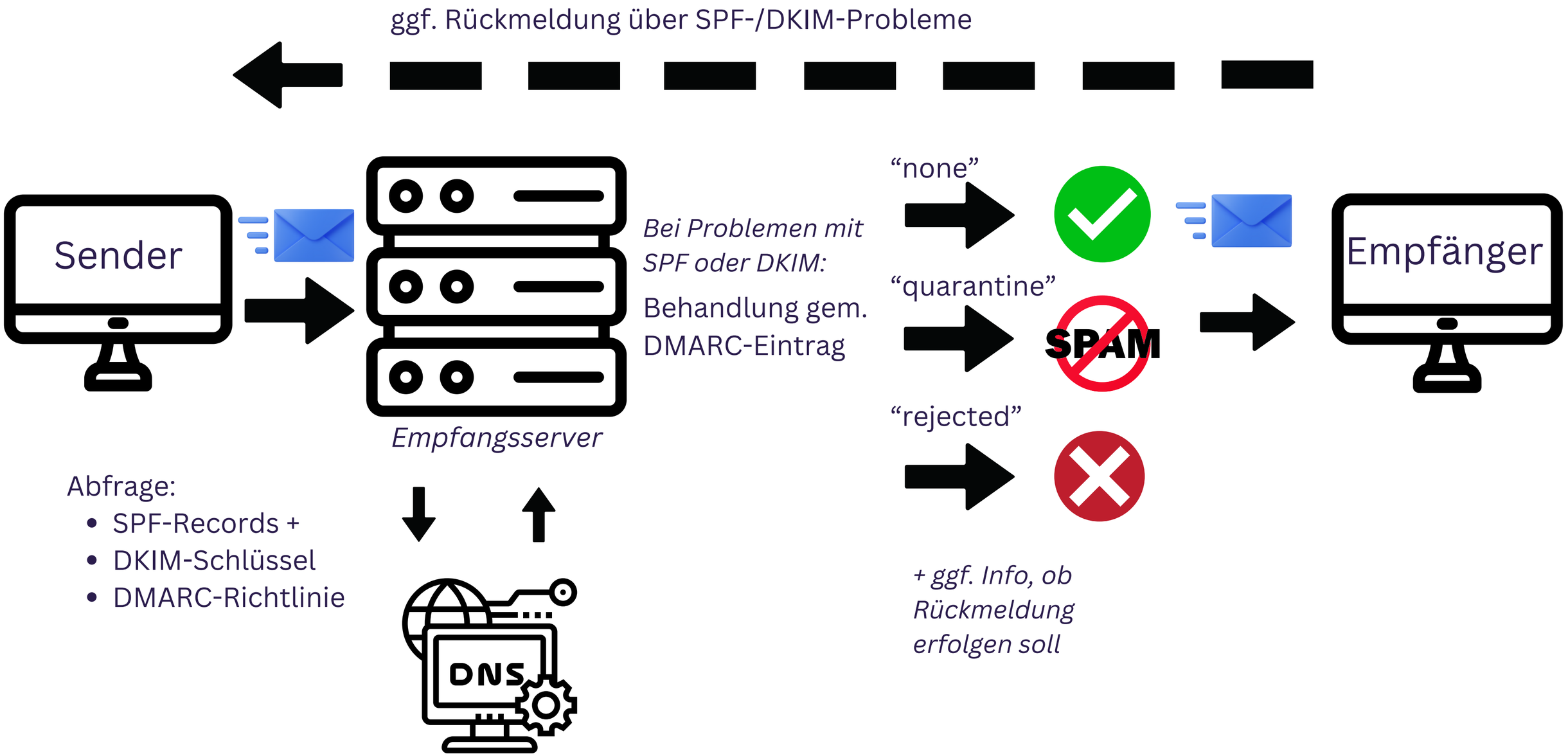
(=Domain-based Message Authentication, Reporting and Conformance)

- Für den Mail-Empfänger: Methode zur E-Mail-Überprüfung
- Für den Mail-Versender: Methode zur Überwachung, welche E-Mails unerlaubterweise mit dem eigenen Absender versandt wurden

Was sind die Vorteile durch DMARC?

- Schutz vor Missbrauch der eigenen Domain (Spoofing)
- Schutz vor Cyberkriminalität (Phishing)
- Erhöhung der Zustellquote beim Versand
  (DMARC wird von manchen Providern vorausgesetzt)

So funktioniert DMARC

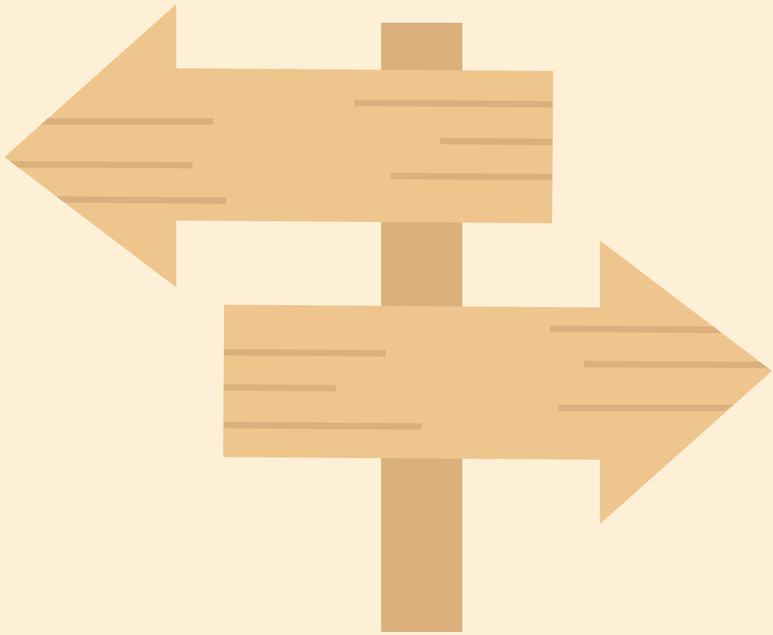


Diese Einstellungen sind wichtig

Für die Absenderdomain beim Mail-Versand ist im DNS zu hinterlegen:

SPF-Records

DKIM-Schlüssel



DMARC-Eintrag

Das bringen SPF, DKIM und DMARC

Verhinderung von Spoofing

Kein Mail-Versand in falschem Namen

Vermeidung von Phishing

Keine Cyberkriminalität durch gefälschte Absender

Bessere Zustellbarkeit von Mails

Viele Provider setzen SPF, DKIM, ggf. DMARC voraus

So richtet man einen DMARC-Eintrag ein

1 Anmeldung beim Domain-Host

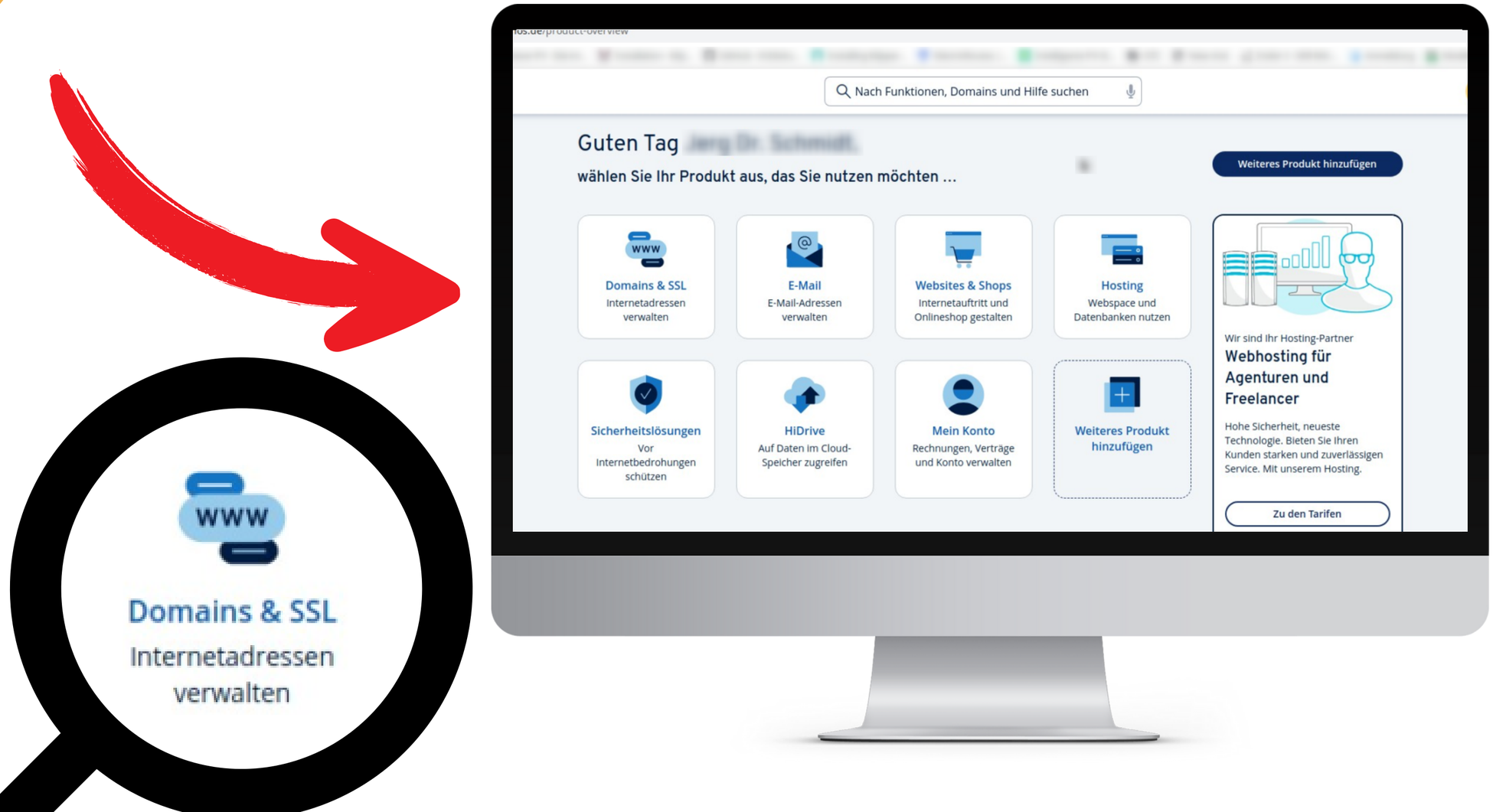
2 TXT Eintrag anlegen:
Hostname: _dmarc.<domainname>

v=DMARC1; p=none;
E-Mail soll trotzdem empfangen werden
v=DMARC1; p=quarantine;
E-Mail soll in Spam-Ordner
v=DMARC1; p=reject;
E-Mail soll nicht angenommen werden

+ ggf. Anweisungen über “Strenge der Prüfung”
+ ggf. Anweisung über Zusendung von Rückmeldungen

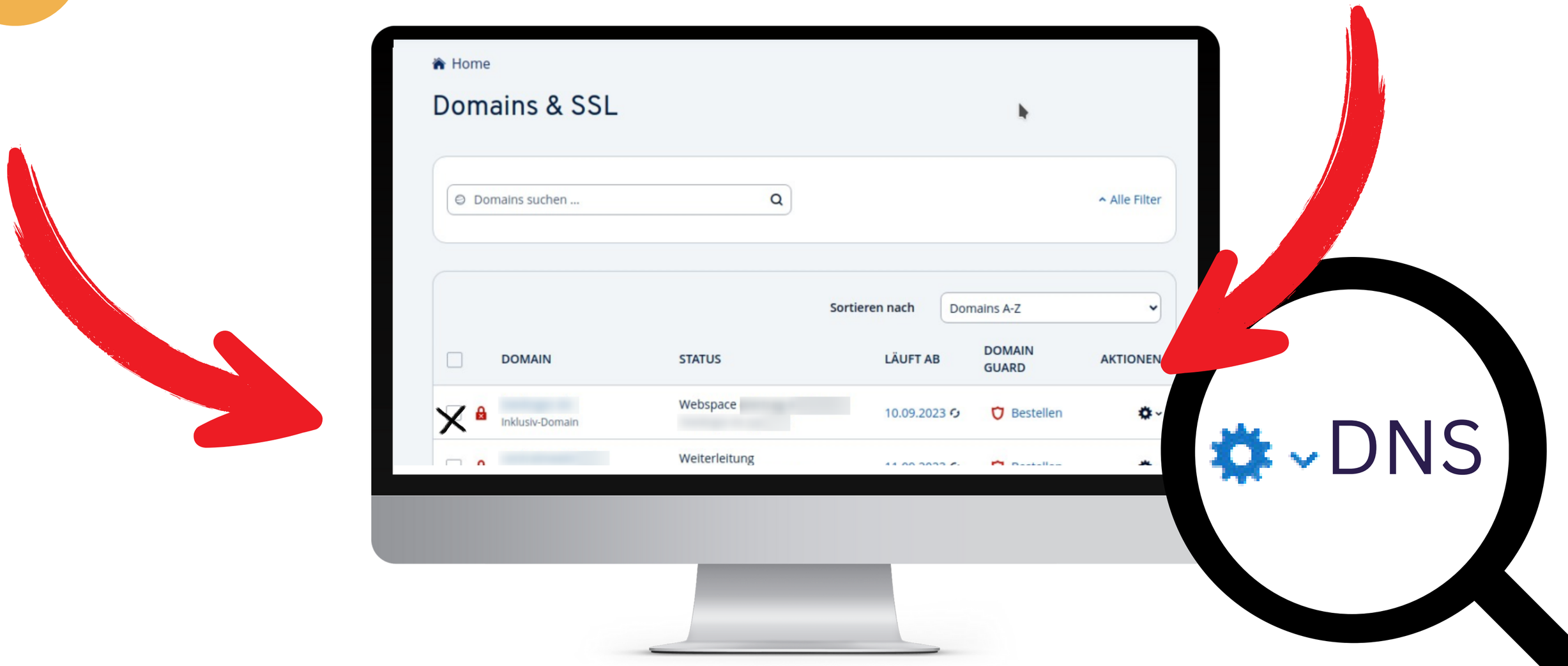
So hinterlegt man einen DMARC-Eintrag z.B. bei 1&1

1 Im Kundenbereich “Domains & SSL” auswählen



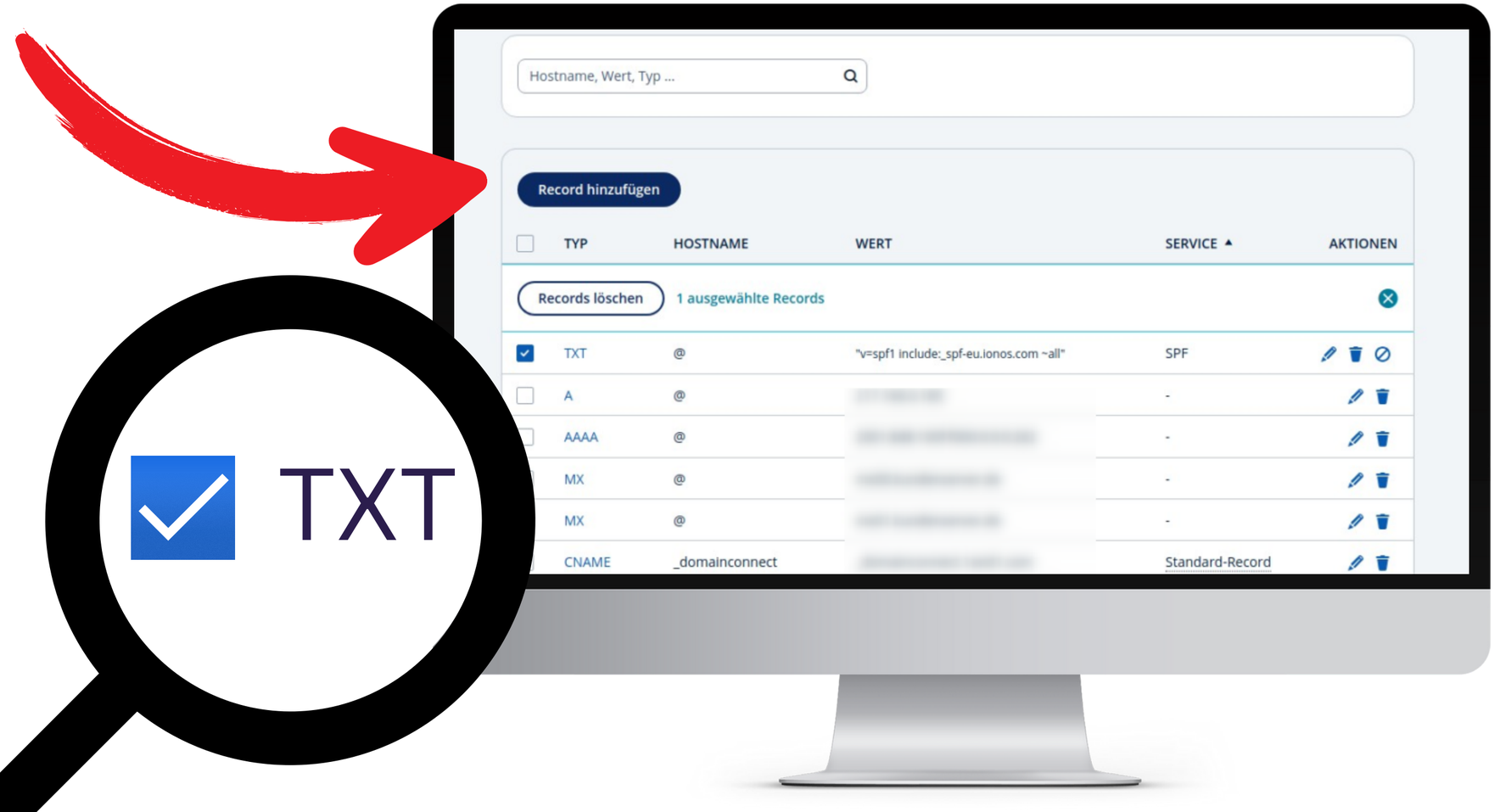
Gewünschte Domain auswählen

2 Absenderdomain auswählen und rechts “DNS” auswählen



Neuen Eintrag anlegen

3 “Record hinzufügen” und “TXT” auswählen



DMARC-Eintrag anlegen

4 Daten für den TXT-Eintrag:

Hostname
(_dmarc.<domainname>)

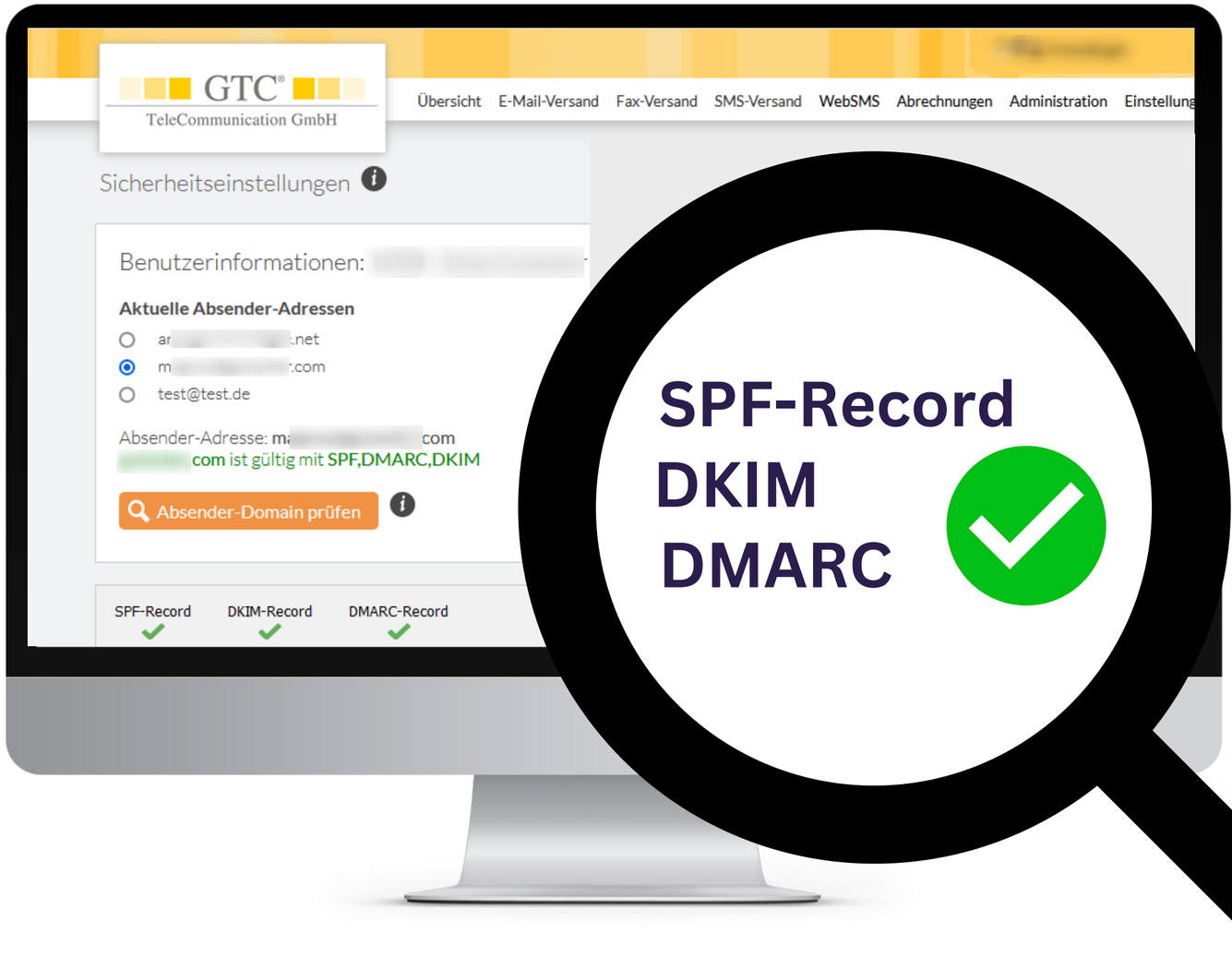
Wert
(v=DMARC1;p=Behandlungswunsch)

None	**quarantine:**	**reject:**
Mails soll zugestellt werden	Mails soll als Spam gewertet werden	Mails sollen nicht angenommen werden

Bsp: Host: _dmarc.beispiel.de
Wert: *v=DMARC1; p=reject*

So versendet man sicher

1. DKIM-Schlüssel bei GTC direkt erzeugen
2. SPF-Record, DKIM und DMARC für die eigene Domain hinterlegen
3. Alle Sicherheitseinstellungen mit einem Klick überprüfen



...und E-Mailings sicher versenden

E-Mailings mit GTC:

- Einfache Gestaltung und Nutzung
- Ohne Grundkosten
- Telefon-Support

www.gtc.de
-> e-mailing

Fragen? Wir helfen Ihnen weiter:
Tel.: **+49(0)711-49090-82** oder
email@gtc.net

GTC®
TeleCommunication GmbH